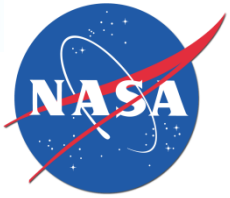
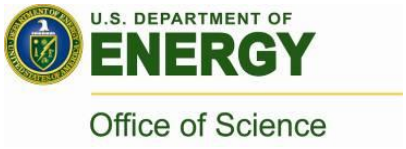
National Privacy Research Strategy Workshop





National Privacy Research Strategy Workshop

Introduction

Tomas Vagoun
NCO/NITRD
vagoun@nitrd.gov
2/18/15

NITRD (Program)

- Purpose
  - The primary mechanism by which the U.S. Government coordinates its unclassified Networking and IT R&D (NITRD) investments
  - Supports NIT-related policy making in the White House Office of Science and Technology Policy (OSTP)
- Scope
  - Approximately $4B/year across 16 agencies, seven program areas
  - Cyber Security and Information Assurance (CSIA)
  - Human Computer Interaction and Information Management (HCI&IM)
  - High Confidence Software and Systems (HCSS)
  - High End Computing (HEC)
  - Large Scale Networking (LSN)
  - Software Design and Productivity (SDP)
  - Social, Economic, and Workforce Implications of IT and IT Workforce Development (SEW)
  - Established by the High-Performance Computing Act of 1991

NPRS Objectives

- WH Office of Science and Technology Policy request to NITRD: prepare a National (Federal) Privacy Research Strategy to:
  - Establish objectives and prioritization guidance for federally-funded privacy research
  - Provide a framework for coordinating R&D in privacy-enhancing technologies
  - Encourage multi-disciplinary research that recognizes the needs of the Government, the needs of the society, and enhances opportunities for innovation in the digital realm

Privacy Policy Context, Examples

- Cybersecurity Enhancement Act of 2014, US Congress
- Big Data: Seizing Opportunities, Preserving Values, The White House, May 2014
- Big Data and Privacy: a Technological Perspective, PCAST, May 2014
- EO 13642: Making Open and Machine Readable the New Default for Government Information, WH, May 2013
- EO 13636: Improving Critical Infrastructure Cybersecurity, WH, Feb 2013
- PPD 21: Critical Infrastructure Security and Resilience, WH, Feb 2013
- Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Consumers, FTC, Mar 2012
- Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, WH, Feb 2012
- U.S. International Strategy for Cyberspace, WH, May 2011
- The National Strategy for Trusted Identities in Cyberspace (NSTIC), WH, Apr 2011
- Commercial Data Privacy and Innovation in the Internet Economy: Dynamic Policy Framework, DOC, Dec 2010
- Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, WH , May 2009
- PCAST reports on the NITRD Program, Jan 2013 and Dec 2010

Privacy Policy Objectives, Examples

- Protect / respect privacy and civil liberties
- Big data analytics to be used in ways that protect civil liberties and privacy rights
- Safeguard individual privacy, confidentiality, and national security
- Develop analysis of privacy, confidentiality, and security risks
- Support Fair Information Practice Principles and the Consumer Privacy Bill of Rights
- Consumers to be able to make decisions about the use of private data; need greater transparency for information collection and use practices
- Need to control the collection and storage of personal data as well as the use of the data and data derived from analytics
- Develop the scientific and engineering foundations of privacy R&D, and the fundamentals of privacy protection and protected disclosure of confidential data

Workshop Objectives

- To surface key privacy perspectives, needs, and challenges that should be considered in forming a privacy research strategy
- To gain a better understanding of what objectives should guide federal privacy research
- To examine prospective research areas that might be used to organize and prioritize federal research in privacy

Workshop Objectives (2)

- Establish a level of understanding/buy-in on the structure of the conversation going forward
  - How to decompose privacy into areas where goals for privacy research could be established
  - How to create a framework that links privacy research objectives into a coherent picture
  - How to formulate research objectives in ways that invite contributions from many disciplines and variety of approaches

Understanding Privacy

- Government Perspective
  - Creating and executing privacy laws/regulations; how to support privacy requirements of such laws; how to conduct law enforcement, national defense while protecting privacy
- Individual Perspective
  - Concerns about the collection and control of personal data and how it is used
- Commerce Perspective
  - Pursuit of business opportunities that involve collection and use of personal information, in marketing, big data analytics, etc.
- Society Perspective
  - Concerns about effects from the loss of privacy on society as a whole, such as erosion of freedom, self-censoring, compartmentalization of people in cyberspace, informational discrimination, etc.
  - How to balance IT innovation with privacy protection

Privacy in the Real World

- One of the ways to think about privacy are concerns about people's ability to avoid harm by being aware of and able to manage what personal information is disclosed, to whom, when, under what circumstances, and for what purposes
- Social and institutional structures create context
- An individual is a member of circles/groups with their own norms

Privacy Groups

- Groups
  - Social (family, friends, etc.), Professional (employment, medical, etc.), Commerce (on-line retail transactions), Government, etc.
  - Groups have different norms/expectations/rules for what is acceptable
  - Group norms may be dynamic
- Violation of privacy
  - Deviations from the norms of a particular group
  - A result of a difference of norms across multiple groups
- Controls
  - Different groups can have varying controls of information flows/disclosures

➢ The social/sociological view of privacy (privacy groups, context) facilitates a natural understanding of privacy

Notional Privacy Research Framework

- Social/sociological privacy model and constructs provide a framework to describe privacy and where research contributions fit
- Research in privacy should lead the way toward the realization of social privacy constructs in cyberspace
- Research themes should identify key gaps in our abilities to realize desired privacy constructs (objects, rules, interactions, controls, etc.) in cyberspace

Privacy Research Areas (proposed)

- Privacy Expectations
  - methods and technologies that will provide the capabilities to define, capture, and operationalize the norms, expectations, and rules for acceptable activities, information disclosure, and data flows in the digital realm
- Privacy Violations
  - methods and technologies for understanding, detecting, assessing, and reasoning about deviations from norms/expectations/rules, and harms
- Privacy Controls
  - methods and technologies to manage and mitigate risk in order to satisfy pertinent privacy norms/expectations/rules and prevent privacy violations

Workshop Structure

- Day-1: needs and challenges in privacy
  - Government, Individual, Commerce, Society perspectives
- Day-2: prospective privacy research areas
  - Privacy expectations, violations, controls
- Day-3: objectives for federal privacy research
  - Future capabilities to be made possible with the research
  - Social needs and values that should guide the research
- Workshop artifacts
  - Workshop summary by Government participants
  - Workshop/NPRS input by R&D community, to be organized by the Computing Community Consortium (CCC)

Tomas Vagoun, PhD
Cybersecurity R&D Technical Coordinator

National Coordination Office for
Networking and Information Technology Research and Development
Suite II-405, 4201 Wilson Blvd.
Arlington, VA 22230
Tel: (703) 292-4873
vagoun@nitrd.gov

http://www.nitrd.gov